THE HONORABLE ROBERT S. LASNIK

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	No. CR19-159-RSL CAPITAL ONE BANK (USA), N.A./CAPITAL ONE FINANCIAL CORP.'S MOTION PURSUANT TO 18 U.S.C. § 3771 Note on Motion Calendar: January 14, 2022

INTRODUCTION

Capital One Bank (USA), N.A. ("Capital One") respectfully submits this memorandum, pursuant to the Crime Victims' Rights Act ("CVRA"), in opposition to Defendant Paige Thompson's Motion to Compel Capital One Data, Dkt. No. 127, and in support of an order, pursuant to Federal Rule of Criminal Procedure 16(d)(1), prohibiting production to the defense team of a complete copy of more than 100,000,000 American and Canadian victims' unredacted personal information.[1]

[1] In a December 22, 2021 filing with this Court, Capital One set forth its concerns with respect to the Defendant's motion to compel, and requested the Court, if necessary, set a briefing schedule on Capital One's CVRA motion. Capital One understands that, due to inclement weather, the courthouse has been closed for several days since that December 22 filing. Accordingly, and in order to preserve and vindicate the victims' rights under the CVRA, Capital One now submits this memorandum in further support of its motion pursuant to the CVRA. If the

DEBEVOISE & PLIMPTON LLP
909 Third Avenue
New York, New York 10022
+1 212 909 6000

What Defendant seeks in her Motion to Compel is as unprecedented as it is dangerous. She demands that she and her legal team be handed the unredacted personal information of tens of millions of the Defendant's victims. Here, the sheer breadth of this demand – the personally identifiable information of more than 100,000,000 individuals – makes it all the more unreasonable. Defendant gives no justification for this demand.

As alleged in the superseding indictment (Dkt. No. 102), the Defendant hacked Capital One in 2019 ("the Hack") and stole data containing the personal details of more than 100,000,000 individuals (the "Consumer Information"). Dkt. No. 102 at 4. The Government seized from the Defendant a computer that contained the Consumer Information. Shortly after the Defendant's arrest, the Government made the Consumer Information available for inspection pursuant to the Federal Rules of Criminal Procedure. More than two years later, defense counsel has yet to inspect it. Dkt. 145 at 1-2.

Nevertheless, defense counsel now asks the Court to compel the Government to furnish to defense counsel a complete copy of the Consumer Information. The wholesale production of more than 100,000,000 records containing the unredacted personal details of the victims is not required under the Federal Rules and would violate the CVRA both by failing to respect the victims' dignity and privacy and by failing to reasonably protect them from the Defendant. Accordingly, the Defendant's motion to compel should be denied in its entirety, and the Court should enter an order restricting the production of unredacted victim information to the Defendant.

I. BACKGROUND

In 2019, the Defendant hacked into Capital One's systems and stole data containing the personal details of some 100,000,000 individuals. Dkt. No. 102 at 4. The Consumer

Defendant's motion to compel is denied, Capital One respectfully submits that there would be no need for the Court to entertain Capital One's CVRA motion.

Information included the personal and financial information of individuals who applied to open credit card accounts with Capital One, or were Capital One customers, including – in some instances – Social Security numbers, Canadian social insurance numbers, and bank account numbers.[2] The information was stored in certain digital containers known as "buckets." In a June 18, 2019 message sent via Twitter, the Defendant made clear the intent behind her crime: She "wanted to distribute those buckets," which she knew contained "ssns…with full name and dob." Dkt. No. 1 at 11. Capital One is aware of no evidence that she distributed the Consumer Information in any way.

Before the Defendant could carry out her plan, however, Capital One was able to identify her and report her conduct to the Federal Bureau of Investigation ("FBI"). The Government seized from the Defendant a computer that contained the Consumer Information. *See* Dkt. No. 1 at 12. The Defendant organized the stolen information – along with her hacking tools – in a computer folder called "aws_hacking_shit." Dkt. No. 145 at 3. In online exchanges, fellow hackers warned the Defendant that she was engaged in "sketchy shit don't go to jail plz." Dkt. No. 1 at 10. The Defendant responded by bragging about her hacking and, in particular, her obfuscation techniques: "Im like > ipredator > s3 on all this shit . . . I wanna get it off my server that's why Im archiving all of it lol." *Id*. iPredator is a reference to a virtual private network, which is a form of obfuscation that hackers can use to hide their digital trail. In light of the Defendant's conduct, she was charged in a superseding indictment returned on June 17, 2021, with wire fraud (18 U.S.C. § 1343), violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), access device fraud (18 U.S.C. § 1029), and aggravated identity theft (18 U.S.C. § 1028A). Dkt. No. 102.

The Government's swift action prevented the Defendant from realizing her plan to

[2] The vast majority of Social Security and bank account numbers (all but roughly 200,000 in total) were tokenized, and therefore unreadable by the Defendant or any other third party.

"distribute th[e] buckets" containing the Consumer Information. Nevertheless, the Defendant's criminal conduct inflicted significant harm on her victims. The Defendant not only victimized the individuals whose personal financial information she stole, but also inflicted significant legal, reputational, and financial harm on Capital One. As of February 25, 2021, Capital One reported that it had incurred $138 million in incremental expenses related to the Hack, largely driven by customer notifications, credit monitoring, technology costs, and legal support.[3] More than 60 consumer complaints were filed against Capital One and consolidated into multi-district consumer litigation. *See In re Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA) (E.D. Va.). Capital One recently announced it settled those claims for $190 million.[4]

Shortly after the Defendant's July 2019 arrest, the Government made, and continues to make, the Consumer Information available for inspection at the Seattle Office of the FBI. *See* Dkt. No. 145 at 9. The Defendant made numerous requests to continue the trial. *See* Dkt. Nos. 60, 78, 82, 89, 93, and 107 (citing the need to review discovery as among the reasons for the continuance). Yet, defense counsel has not even inspected the Consumer Information. Dkt. 145 at 1-2.

Instead, the Defendant now insists that the Government produce to defense counsel a complete copy of the data the Defendant allegedly stole to enable "continuous, uninterrupted, and confidential access to the data that is not logged by the FBI and shared with government attorneys." Dkt. No. 127 at 5. The Government has attempted to find suitable solutions to these concerns. *See* Dkt. No. 127, Exs. 1 & 2. Among other things, the Government proposed

[3] Capital One, Annual Report (Form 10-K), 6 (Feb. 25, 2021), available at https://investor.capitalone.com/sec-filings/sec-filing/10-k/0000927628-21-000094.

[4] *Id.* at Dkt. 2204. Capital One Financial agreed to pay $190 million to settle customer lawsuit over cyberattack, WASH. POST, Dec. 23, 2021, available at https://www.washingtonpost.com/business/economy/capital-one-financial-agreed-to-pay-190-million-to-settle-customer-lawsuit-over-cyberattack/2021/12/23/fa69348c-63e8-11ec-bf70-58003351c627_story.html.

DEBEVOISE & PLIMPTON LLP
909 Third Avenue
New York, New York 10022
+1 212 909 6000

that defense counsel first inspect the data at the FBI's offices to identify what specific files (if any) defense counsel wishes to copy. The Government has stated that it would "be happy at that stage to discuss producing some much smaller sample of the data stolen by [Defendant], perhaps in redacted form." Dkt. No. 127, Ex. 2 at 2. The Defendant has refused even this suggestion as "logistically unfeasible." Dkt. No. 127 at 5.

In a letter to the Government dated November 30, 2021, Capital One described its concerns with, and objected to, a wholesale production of the stolen Consumer Information to the Defendant. Dkt. No. 145, Ex. 2. In a December 22, 2021 filing with this Court, Capital One set forth its concerns, and requested, if necessary, a briefing schedule on its CVRA motion. In order to preserve and vindicate victims' rights under the CVRA, Capital One now submits this memorandum in further support of its CVRA motion.

II. ARGUMENT

A. The Court Has Jurisdiction Under The CVRA

The Court has jurisdiction over Capital One's CVRA motion because it is "the district court in which [the] defendant is being prosecuted." 18 U.S.C. § 3771(d)(3). The CVRA authorizes "crime victims" or their "lawful representative" to bring motions to vindicate victims' rights. 18 U.S.C. § 3771(d). Where "the number of crime victims makes it impracticable to accord all of the crime victims the rights described in [the CVRA]," the statute directs that "the court shall fashion a reasonable procedure to give effect to this chapter that does not unduly complicate or prolong the proceedings." 18 U.S.C. § 3771(d)(2).

Capital One and the individuals whose personal details were contained in the stolen Consumer Information are plainly victims under the CVRA because they were "directly and proximately harmed as a result of the commission of" the Defendant's criminal conduct. 18 U.S.C. § 3771(e)(2)(A). Victims of theft fit comfortably within the broad definition of a

"crime victim" under the CVRA given that "a party may qualify as a victim, even though it may not have been the target of the crime, as long as it suffers harm as a result of the crime's commission." *United States v. Ruzicka,* 331 F. Supp. 3d 888, 894 (D. Minn. 2018) (citing *In re Stewart*, 552 F.3d 1285, 1289 (11th Cir. 2008)); *Moore v. United States*, 178 F.3d 994, 1001 (8th Cir. 1999) (holding that a bystander of a bank robbery was a victim under the closely-related Mandatory Victims Restitution Act); *see also Ruzicka*, 331 F. Supp. 3d at 898 (finding corporation was a victim for purposes of the CVRA). Here, of course, the Defendant specifically targeted Capital One and the data containing personal details of more than 100,000,000 individuals; if convicted, the Defendant likely will owe restitution to Capital One as well as those individuals. *See* 18 U.S.C. § 3663A.

B. Wholesale Production Of The Unredacted Consumer Information Violates Victims' Rights By Re-Victimizing Them and Is Not Required Under The Federal Rules

1. The Government Has Already Discharged Its Rule 16 Obligations

Shortly after the Defendant's arrest in July 2019, the Government made the Consumer Information available for inspection by the defense team at the FBI's Seattle offices. The Government therefore has fully discharged its obligations under Federal Rule of Criminal Procedure 16, which requires the Government to "permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, [and] tangible objects . . . within the government's possession." Fed. R. Crim. P. 16(a)(1)(e).

It is the Defendant – not the Government – that has refused to comply with Rule 16. The Defendant insists that Rule 16 requires wholesale production of the unredacted records containing the personal details of the Defendant's victims. The Defendant is incorrect as a matter of law. "The language of Rule 16 does not require production. Instead, Rule 16 says the Government must make relevant materials 'available for inspection, copying, or

photographing[.]'" *United States v. Pac. Gas & Electric Co.*, No. 14-CR-00175-TEH, 2015 WL 3958111, at *14 (N.D. Cal. June 29, 2015).[5]

In *PG&E*, the defendant argued Rule 16 required the Government to produce copies of – not merely make available for inspection – certain notes "so that the notes are 'readily available for trial preparation and trial examinations.'" *Id.* at *14. That argument is nearly identical to the Defendant's instant assertion that her "legal team needs continuous, uninterrupted, and confidential access to the data that is not logged by the FBI and shared with government attorneys." Dkt. No. 127 at 5 (asserting inspection at the FBI's offices is "logistically unfeasible"). In rejecting the defendant's demand for production of the notes in *PG&E*, the court held that "PG & E's attorneys can review the requested documents at the U.S. Attorney's Office and request official copies of any specific documents it intends to use at trial, as suggested by the Government." *Pac. Gas & Electric Co.*, 2015 WL 3958111, at *14. That is precisely what the Government has offered as the path forward here. Dkt. No. 127, Ex. 2 at 2. Rule 16 prescribes this process so that the Government (and, if necessary, the victims) may review the proposed discovery; assess whether redactions or other protective measures are needed; and present a narrowed set of disputed issues and documents to this Court for adjudication. This process conserves judicial resources while balancing the valid rights of the Defendant, the Government, and the victims.

2. Producing the Consumer Information to Defendant Would Contravene the Protections of the CVRA

As crime victims, Capital One and the individuals whose personal details the Defendant stole have the "unquestionable right" to be "reasonably protected from the accused" and "to be treated with fairness and with respect for [their] dignity and privacy." 18 U.S.C. §

[5] Though the court cited Rule 16(a)(1)(B) in reaching this conclusion, the court's decision more generally analyzes the Government's obligations pursuant to Rule 16. *See, e.g.*, *id.* at *1.

3771(a)(1), (8); *United States v. Patkar*, Cr. No. 06-00450 JMS, 2008 WL 233062, at *5 (D. Haw. Jan. 28, 2008). The Defendant surreptitiously and without authorization hacked into Capital One's protected systems; stole the Consumer Information; messaged on Twitter about her plan to "distribute" it; and bragged online about the steps she had taken to avoid detection and capture. A few weeks after the Defendant told others of her plan to "distribute those buckets" and mere days after Capital One reported her conduct to the FBI, the Government arrested the Defendant and interrupted her plans to disseminate the data.

The Defendant asks this Court to order the Government to go above and beyond its discovery obligations and disseminate to defense counsel the very information that Defendant stole and intended to "distribute" as part of her criminal scheme. Granting such an order would re-victimize the victims by once again putting their unredacted data in the hands of the Defendant's representatives. The Consumer Information includes personal details of more than 100,000,000 individuals; it was the object of the Defendant's criminal conduct; and the computer on which it was stored is subject to forfeiture. Courts routinely deny requests to compel the Government to produce such contraband to defendants. *See, e.g.*, *United States v. Benzer*, No. 213-CR-00018-JCMGWF, 2015 WL 9200365, at *7 (D. Nev. Dec. 15, 2015) (In the context of a third-party challenge to it, approving a protective order that permitted defendant to inspect documents containing sensitive personal information, and to obtain copies of relevant material only upon motion to the court); *United States v. Husband*, 246 F. Supp. 2d 467, 469 (E.D. Va. 2003) (Government satisfied its discovery obligations by making videotape available for inspection; procedure established to permit anonymous access by defense expert).

Imposing the exceptional discovery requirement of ordering the wholesale production of the unredacted Consumer Information under these circumstances would violate the CVRA by unnecessarily infringing on the dignity and privacy of the victims. Moreover, it imposes on

the victims the risk that their data will be disseminated. An order that requires the Government to go beyond its discovery obligations and imposes this substantial burden on the victims falls far short of treating them "with fairness," as is required under the CVRA. 18 U.S.C. § 3771(a)(8); *see also United States v. Turner,* 367 F. Supp. 2d 319, 335 (E.D.N.Y. 2005) (holding courts must apply a "liberal reading of the statute in favor of interpretations that promote victims' interest in fairness, respect, and dignity" because the CVRA was meant "to correct, not continue, the legacy of the poor treatment of crime victims in the criminal process").

Though the Defendant argues that the Government sometimes produces sensitive information to the Federal Public Defender's Office pursuant to protective orders, the Defendant's request to do so here is materially different for at least four reasons: (1) the sheer volume of the discovery involved; (2) the Defendant's refusal to comply with the process set forth in Rule 16; (3) the Defendant's prior declaration that she intends to disseminate the Consumer Information; and (4) the status of the Consumer Information as contraband, not merely evidence of the Defendant's crimes. Particularly where, as here, the Government has set forth the reasons why this information is unlikely to be material to the trial, the existence of the protective order cannot justify imposing an unfair burden on the victims that their unredacted data may be disseminated. Dkt. No. 145 at 6. Accordingly, the Defendant's request to impose enhanced discovery obligations on the Government should be denied as it violates the CVRA.

C. Wholesale Production Of The Unredacted Consumer Information Fails To Protect The Dignity and Privacy Of The Victims And Fails To Reasonably Protect Them From The Defendant

Even if the Defendant's request comported with Rule 16 (and it does not), it would still violate the victims' rights to be treated with respect for their dignity and privacy, and to be reasonably protected from the Defendant. *See* 18 U.S.C. § 3711(a)(1), (8). If the Defendant's motion is granted, the Government would be forced to turn over the unredacted personal details of more than 100,000,000 victims. The Defendant provides no justification for this demand. The conclusory assertion that it would be "logistically unfeasible" to inspect the data at the FBI's offices certainly does not suffice; "[l]ogistical issues do not entitle Defendant to unredacted discovery." *United States v. Gatewood*, No. CR 11–08074–PCT–JAT, 2012 WL 2286999, at *2 (D. Ariz. June 18, 2012). There is "no duty on the Government to disclose all information . . . ." *Id*. In fact, as the *Gatewood* court recognized, the CVRA imposes "a duty to withhold much of the . . . information on privacy grounds." *Id*. (citing 18 U.S.C. § 3771(a)(8)).

Aside from purported logistical issues that plainly do not outweigh the victims' rights, the Defendant contends, again in conclusory fashion, that the Consumer Information is "part and parcel of the government's case-in-chief and material to Ms. Thompson's defense." Dkt. No. 127 at 2. In short, the claim that the information is "material" to the defense does not suffice to overcome victims' rights, particularly when sensitive financial information is involved. *See* Dkt. No. 145 at 6-7 (describing why the Consumer Information is not material to the prosecution or defense). The court faced a similar situation in *United States v. Jenkins*, No. 2:07–cr–00080–RCJ–PAL, 2009 WL 10678771, at *1-2 (D. Nev. Apr. 2, 2009). There, defendant sought to compel the Government to obtain and produce bank account information associated with a victim. In opposition, the Government cited the CVRA's requirement that

victims be treated with respect for the dignity and privacy of their information. *Id*. at *1. The court agreed, holding that it was "not persuaded that the defendants are entitled to review the victim's private and sensitive banking records for the stated purpose of determining whether the funds the victim alleges the defendants defrauded him out of were actually his funds." *Id*. at *2. The situation here is even more compelling because the Defendant has failed to articulate *any* reason why it needs a complete, unredacted copy of more than 100,000,000 records containing sensitive details about the Defendant's victims. *See, e.g.*, *Gatewood*, 2012 WL 2286999, at *1 (production denied where "Defendant will not give more justification for his request because Defendant claims that doing so would be impossible 'without revealing the nature of the defense investigation, the strategy of the defense, and potential defenses at trial.'").

Granting the Defendant's motion would also fail to reasonably protect the victims from the Defendant. Courts have recognized a heightened need to protect victims from defendants who have been shown to abuse personal information. *See, e.g.*, *United States v. Dixon*, 355 F. Supp. 3d 1, 4-8 (D.D.C. 2019) (where defendant used personal information to lure a victim to a gunpoint robbery, order withholding "sensitive or personally identifying information about witnesses from" defendant was appropriate); *United States v. Torres*, No. 20-CR-00418, 2020 WL l4500046, at *5 (D.N.J. Aug. 4, 2020) (approving process where defense team could inspect but not possess "protected information" because "[f]urther dissemination of [explicit] photographs is likely to cause further embarrassment and humiliation to the alleged victims"). Here, the Defendant declared her intentions clearly: to "distribute those buckets" that contained personal details of more than 100,000,000 individuals. To now give back to the Defendant's representatives a complete, unredacted copy of that data fails to reasonably protect the victims from the Defendant. Accordingly, there is good cause to deny the

Defendant's motion to compel and to enter an order, pursuant to Rule 16(d)(1), restricting the production of this sensitive data.

CONCLUSION

The Defendant's sweeping demand for wholesale production of the unredacted Consumer Information should be denied because it violates the CVRA. The Defendant has failed to follow the process prescribed by Rule 16 to inspect the data, and seeks instead to impose additional burdens on the Government at the cost of the victims of her alleged crimes. The provision of a complete copy of more than 100,000,000 unredacted records containing personal details of individuals victimized by the Defendant's conduct would not treat those victims fairly; would not respect their dignity and privacy; and would not reasonably protect them from the Defendant, all in violation of the CVRA. Accordingly, the Defendant's motion to compel should be denied in its entirety, and an order entered pursuant to Rule 16(d)(1) restricting the production of the unredacted Consumer Information.[6]

Respectfully submitted this 31st day of December, 2021.

DEBEVOISE & PLIMPTON LLP

s/John Gleeson
s/James J. Pastore
John Gleeson
James J. Pastore, Jr.
919 Third Avenue
New York, NY 10022
Telephone: (212) 909-6000
Attorneys for Capital One

ORRICK, HERRINGTON & SUTCLIFFE LLP

s/Aravind Swaminathan
Aravind Swaminathan, WSBA #33883
701 Fifth Avenue
Suite 5600
Seattle, WA 98104-7097
Telephone: (206) 839-4300
Attorney for Capital One

[6] To the extent the Court intends to order the wholesale production of 100,000,000 unredacted records to the defense team, Capital One respectfully requests that the Court order the parties to confer on the safeguards to be applied to those records, including the possibility of Capital One hosting the data on its premises, or the premises of one or more of its law firms at locations convenient to defense counsel's offices.